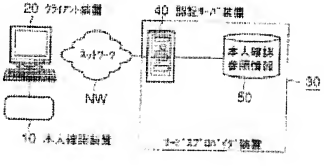
PERSONAL AUTHENTICATION SYSTEM AND PROGRAM

Publication number: JP2003224562 (A)
Publication date: 2003-08-08
Inventor(s): IKEDA TATSURO; MORIJIRI TOMOAKI; SAISHIYO TOSHIAKI
Applicant(s): TOKYO SHIBAURA ELECTRIC CO
Classification:
- international: ***H04L9/32;*** **H04L9/32;** (IPC1-7): H04L9/32
- European:
Application number: JP20020019030 20020128
Priority number(s): JP20020019030 20020128

Abstract of **JP 2003224562 (A)**

PROBLEM TO BE SOLVED: To block impersonation by a third person at the time of secret communication. ; SOLUTION: A client device 2 uses the message of the agreement processing of the secret communication and transmits individual confirmation specifications regarding personal authentication of a user to an authentication server device 40. The authentication server device 40 selects personal confirmation specification matched with the security policy of the present device among the transmitted individual confirmation specifications and returns an obtained selected result. The client device notifies the authentication server device of the obtained individual confirmation information of the user in a ciphered state based on the returned selected result regarding the individual confirmation specification. The authentication server device deciphers the ciphered individual confirmation information, executes an individual confirmation processing on the basis of an obtained deciphered result and interrupts the agreement processing of the secret communication when the individual confirmed result indicates dishonesty. ;



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－224562
（Ｐ2003－224562Ａ）
(43)公開日　平成15年８月８日(2003.8.8)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｃ　５Ｊ１０４

審査請求　未請求　請求項の数９　ＯＬ　（全 14 頁）

(21)出願番号　特願2002－19030(Ｐ2002－19030)

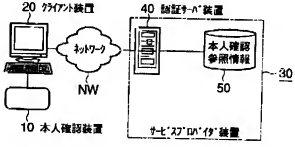
(22)出願日　平成14年１月28日(2002.1.28)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　池田　竜朗
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(72)発明者　森尻　智昭
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　個人認証システム及びプログラム

(57)【要約】
【課題】　秘匿通信の際に、第三者の成り済ましを阻止する。
【解決手段】　クライアント装置２０は、秘匿通信の合意処理のメッセージを用い、ユーザの個人認証に関する本人確認仕様を認証サーバ装置４０に送信する。認証サーバ装置４０は、送信された本人確認仕様のうち、自装置のセキュリティポリシーに合致した本人確認仕様を選択し、得られた選択結果を返信する。クライアント装置は、返信された本人確認仕様に関する選択結果に基づき、得られたユーザの本人確認情報を暗号化した状態で認証サーバ装置に通知する。認証サーバ装置は、この暗号化された本人確認情報を復号し、得られた復号結果に基づいて本人確認処理を実行し、この本人確認結果が不正を示すとき、秘匿通信の合意処理を中断する。



【特許請求の範囲】

【請求項１】　第１エンティティ装置と第２エンティティ装置との間でネットワークを介して秘匿通信をする際に、前記第１エンティティ装置のユーザを前記第２エンティティ装置が個人認証する個人認証システムであって、

前記第１エンティティ装置は、

前記秘匿通信の合意処理のメッセージを用い、前記ユーザの個人認証に関する本人確認仕様を前記第２エンティティ装置に送信する手段と、

この送信された本人確認仕様に関する前記第２エンティティ装置の選択結果に基づき、得られた前記ユーザの本人確認情報を暗号化した状態で前記第２エンティティ装置に通知する手段とを備え、

前記第２エンティティ装置は、

前記第１エンティティ装置から送信された本人確認仕様のうち、自装置のセキュリティポリシーに合致した本人確認仕様を選択し、得られた選択結果を前記第１エンティティ装置に送信する手段と、

前記第１エンティティ装置から通知された暗号化された本人確認情報を復号し、得られた復号結果に基づいて本人確認処理を実行する手段と、

この本人確認処理による本人確認結果が不正を示すとき、前記合意処理を中断する手段とを備えたことを特徴とする個人認証システム。

【請求項２】　第１エンティティ装置と第２エンティティ装置との間でネットワークを介して秘匿通信をする際に、前記第１エンティティ装置のユーザを個人認証する第２エンティティ装置に用いられる個人認証プログラムであって、

前記第２エンティティ装置のコンピュータを、

前記秘匿通信の合意処理のメッセージを用いて前記第１エンティティ装置から送信された前記ユーザの個人認証に関する本人確認仕様のうち、自装置のセキュリティポリシーに合致した本人確認仕様を選択し、得られた選択結果を前記第１エンティティ装置に送信する手段、

この送信された選択結果に基づいて前記第１エンティティ装置から通知された暗号化された状態の本人確認情報を復号し、得られた復号結果に基づいて本人確認処理を実行する手段、

この本人確認処理による本人確認結果が不正を示すとき、前記合意処理を中断する手段、

として機能させるための個人認証プログラム。

【請求項３】　第１エンティティ装置と第２エンティティ装置との間でネットワークを介して秘匿通信をする際に、前記第１エンティティ装置のユーザを前記第２エンティティ装置に個人認証させるための個人認証プログラムであって、前記第１エンティティ装置のコンピュータを、

前記秘匿通信の合意処理のメッセージを用い、前記ユーザの個人認証に関する本人確認仕様を前記第２エンティティ装置に送信する手段、

この送信された本人確認仕様に関する前記第２エンティティ装置の選択結果に基づき、得られた前記ユーザの本人確認情報を暗号化した状態で前記第２エンティティ装置に通知する手段、

この通知した本人確認情報を前記第２エンティティ装置が不正と判定し、前記合意処理の中断宣言を返信したとき、前記中断宣言を出力する手段、

として機能させるための個人認証プログラム。

【請求項４】　第１エンティティ装置が通信代理装置及びネットワークを介して第２エンティティ装置との間で秘匿通信をする際に、前記第１エンティティ装置のユーザを前記通信代理装置を介して認証代理装置が個人認証する個人認証システムであって、

前記第１エンティティ装置は、

前記秘匿通信の合意処理のメッセージを用い、前記ユーザの個人認証に関する本人確認仕様を前記通信代理装置に送信する手段と、

この送信された本人確認仕様に対応して得られる前記ユーザの本人確認情報を暗号化した状態で前記通信代理装置に通知する手段とを備え、

前記通信代理装置は、

前記第１エンティティ装置から送信された本人確認仕様を前記認証代理装置に送信する手段と、

この送信された本人確認仕様に関する前記認証代理装置の選択結果に基づき、前記第１エンティティ装置から通知された暗号化された本人確認情報を前記認証代理装置に送信する手段と、

前記認証代理装置から送信された本人確認結果が不正を示すとき、前記合意処理を中断する手段とを備え、

前記認証代理装置は、

前記通信代理装置から送信された本人確認仕様のうち、予め設定されたセキュリティポリシーに合致する本人確認仕様を選択し、得られた選択結果を前記通信代理装置に送信する手段と、

前記通信代理装置から通知された暗号化された本人確認情報を復号し、得られた復号結果に基づいて本人確認処理を実行し、得られた本人確認結果を前記通信代理装置に送信する手段とを備えたことを特徴とする個人認証システム。

【請求項５】　請求項４に記載の個人認証システムにおいて、

前記認証代理装置は、前記セキュリティポリシーに合致する複数の本人確認仕様を選択することを特徴とする個人認証システム。

【請求項６】　第１エンティティ装置が通信代理装置及びネットワークを介して第２エンティティ装置との間で秘匿通信をする際に、前記第１エンティティ装置のユーザを認証代理装置に個人認証させるための前記通信代理

装置に用いられる個人認証プログラムであって、
前記通信代理装置のコンピュータを、
前記秘匿通信の合意処理のメッセージを用いて前記第１エンティティ装置から送信された前記ユーザの個人認証に関する本人確認仕様を前記認証代理装置に送信する手段、
この送信された本人確認仕様に関する前記認証代理装置の選択結果に基づき、前記第１エンティティ装置から通知された暗号化された本人確認情報を前記認証代理装置に送信する手段、
前記認証代理装置から送信された本人確認結果が不正を示すとき、前記合意処理を中断する手段、
として機能させるための個人認証プログラム。
【請求項７】　第１エンティティ装置が通信代理装置及びネットワークを介して第２エンティティ装置との間で秘匿通信をする際に、前記第１エンティティ装置のユーザを前記通信代理装置を介して個人認証する認証代理装置に用いられる個人認証プログラムであって、
前記認証代理装置のコンピュータを、
前記秘匿通信の合意処理のメッセージを用いて前記第１エンティティ装置から送信されて前記通信代理装置から受信した前記ユーザの個人認証に関する本人確認仕様のうち、予め設定されたセキュリティポリシーに合致する本人確認仕様を選択し、得られた選択結果を前記通信代理装置に送信する手段、
この送信された本人確認仕様に対応して得られる前記ユーザの本人確認情報が暗号化された状態で前記第１エンティティ装置から送信されて前記通信代理装置から通知されると、当該暗号化された本人確認情報を復号し、得られた復号結果に基づいて本人確認処理を実行し、得られた本人確認結果を前記通信代理装置に送信する手段、
として機能させるための個人認証プログラム。
【請求項８】　請求項７に記載の個人認証プログラムにおいて、
前記通信代理装置から受信した本人確認仕様が複数個あるとき、前記セキュリティポリシーに合致する複数の本人確認仕様を選択することを特徴とする個人認証プログラム。
【請求項９】　第１エンティティ装置が通信代理装置及びネットワークを介して第２エンティティ装置との間で秘匿通信をする際に、前記第１エンティティ装置のユーザを前記通信代理装置を介して認証代理装置に個人認証させるための個人認証プログラムであって、
前記第１エンティティ装置のコンピュータを、
前記秘匿通信の合意処理のメッセージを用い、前記ユーザの個人認証に関する本人確認仕様を前記通信代理装置に送信する手段、
この送信された本人確認仕様に対応して得られる前記ユーザの本人確認情報を暗号化した状態で前記通信代理装置に通知する手段、
この通知した本人確認情報に基づいて前記認証代理装置から前記通信代理装置に送信された本人確認結果が不正を示し、前記通信代理装置から前記合意処理の中断宣言を受信したとき、この中断宣言を出力する手段、
として機能させるための個人認証プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信相手の認証に用いられる個人認証システムに係わり、特に、機器認証を行なう秘匿通信合意処理の最中に、個人認証を行なうことにより、成り済ましを阻止し得る個人認証システム及びプログラムに関する。
【０００２】
【従来の技術】近年、インターネットの普及に伴い、オープンな環境での通信が一般的になり、通信経路上での通信の保護が求められてきている。インターネットにおけるWWW（World Wide Web）システムなどでは、WWWクライアント装置とWWWサーバ装置との間の通信を保護する場合、一般に、秘匿通信プロトコルが用いられる。
【０００３】秘匿通信プロトコルは、主に通信内容の秘匿、通信相手の認証、通信内容の認証、及び暗号化鍵の交換等を統合的に処理するための通信規約である。具体的にはＳＳＬ（Secure Sockets Layer）、ＴＬＳ（Transport Layer Security）及びＳ－ＨＴＴＰ（Secure HTTP）等がある。
【０００４】例えばＳＳＬ又はＴＬＳは、ＯＳＩ（Open Systems Interconnection）７層モデルのセッション層を対象とし、機器内などに保存した公開鍵証明書に基づいて通信相手を認証することにより、上位層に対して透過的な秘匿通信を提供している。係るＳＳＬ及びＴＬＳは、標準的な秘匿通信プロトコルとして広く普及している。
【０００５】また、ＯＳＩ７層モデルのネットワーク層を対象とし、における通信プロトコルであるＩＰ（Internet Protocol）を対象とした秘匿通信としてＩＰｓｅｃ（IP Security Protocol）がある。このＩＰｓｅｃは、ＩＰパケットレベルでの認証及び暗号化のための通信規約であり、ホスト単位での秘匿通信を実現し、ＶＰＮ（Virtual Private Network）等に利用される。
【０００６】一方、以上のような通信自体を保護する秘匿通信プロトコルとは異なり、個人自体を認証・確認手段として、生体情報を用いた生体認証（バイオメトリクス）がある。生体認証は、認証時に測定した個人の生体的特徴を示す測定情報と、事前に登録した本人の生体的特徴を示す生体情報とを照合し、認証対象が本人か否かを判断する技術である。
【０００７】ここで、生体的特徴としては、指紋、虹彩、網膜、顔、音声、キーストローク、サイン等の如き、本人固有のものであり且つ複製困難なものが利用さ

れる。よって、生体認証では、第三者による成り済ましが困難となっている。

【0008】従って、現状の個人認証システムでは、秘匿通信プロトコルにより構築した通信路を伝送経路として、生体認証の測定情報を送信することにより、伝送経路上の測定情報等を保護しつつ、生体認証により第三者の成り済ましを阻止可能となっている。

【0009】

【発明が解決しようとする課題】しかしながら、以上のような個人認証システムでは、一般的には問題が無いようであるが、本発明者の考察によれば、以下のような可能性が考えられる。すなわち、ユーザ個人を認証するタイミングは生体認証の時であるので、秘匿通信プロトコルによる秘匿通信合意処理時には、成り済ましが可能である。

【0010】例えばSSL／TLSは、公開鍵証明書に基づいて通信相手を認証している。また、公開鍵証明書は、発行対象となるエンティティ装置（この場合、クライアント装置）の正当性を証明するものである。従って、正当なクライアント装置を使用した第三者の成り済ましの場合、通信相手の認証の際に、否認できずに成り済ましが可能となる。このため、ユーザ個人と公開鍵証明書及び秘密鍵とを一致させるように秘密鍵などを管理する必要があると考えられる。

【0011】これは、公開鍵暗号方式以外の認証方式にも該当することであり、認証判断の基となる情報自体の信頼性が重要となる。すなわち、既知共有情報（既知共有鍵、パスワードなど）に基づいた認証方式では、既知共有情報の安全な管理が重要であり、公開鍵暗号方式に基づいた認証方式では、秘密鍵などの安全な管理が重要である。

【0012】しかしながら、複数ユーザが使用するパーソナルコンピュータのような機器環境においては、安全に管理された既知共有情報や秘密鍵などの秘密情報によっても、ユーザ個人を確認することは困難である。例えば、機器の管理者権限を持つものは、機器内に保存された公開鍵証明書及び秘密鍵等の秘密情報にアクセスし、所望のユーザに成り済ますことが可能である。

【0013】一方、ユーザ個人と秘密情報とを一致させる管理の例として、秘密情報が格納されたICカードの如きセキュア媒体をユーザ個人に携帯させる方式がある。しかしながら、この方式でも、セキュア媒体を不正に持ち出した管理者などにより、同様に成り済ましが可能である。

【0014】従って、現状の個人認証システムとしては、前述した通り、秘匿通信プロトコルによる秘匿通信合意処理の後に、生体認証による個人認証を行なう方式が考えられている。しかしながら、本発明者の考察によれば、秘匿通信合意処理時に成り済ましが可能であれば、成り済ましをした者により、何らかの不正な処理が行われる心配がある。

【0015】本発明は上記実情を考慮してなされたもので、秘匿通信の際に、第三者の成り済ましを阻止し得る個人認証システム及びプログラムを提供することを目的とする。

【0016】

【課題を解決するための手段】第1の発明は、第1エンティティ装置と第2エンティティ装置との間でネットワークを介して秘匿通信をする際に、前記第1エンティティ装置のユーザを前記第2エンティティ装置が個人認証する個人認証システムを対象とする。

【0017】ここで、前記第1エンティティ装置は、前記秘匿通信の合意処理のメッセージを用い、前記ユーザの個人認証に関する本人確認仕様を前記第2エンティティ装置に送信する手段と、この送信された本人確認仕様に関する前記第2エンティティ装置の選択結果に基づき、得られた前記ユーザの本人確認情報を暗号化した状態で前記第2エンティティ装置に通知する手段とを備えている。

【0018】また、前記第2エンティティ装置は、前記第1エンティティ装置から送信された本人確認仕様のうち、自装置のセキュリティポリシーに合致した本人確認仕様を選択し、得られた選択結果を前記第1エンティティ装置に送信する手段と、前記第1エンティティ装置から通知された暗号化された本人確認情報を復号し、得られた復号結果に基づいて本人確認処理を実行する手段と、この本人確認処理による本人確認結果が不正を示すとき、前記合意処理を中断する手段とを備えている。

【0019】従って、第1の発明は以上のような手段を講じたことにより、接続してきたユーザが本人か否かを秘匿通信合意処理段階において確認できるので、秘匿通信の際に、第三者の成り済ましを阻止することができる。

【0020】一方、第2の発明は、第1エンティティ装置が通信代理装置及びネットワークを介して第2エンティティ装置との間で秘匿通信をする際に、前記第1エンティティ装置のユーザを前記通信代理装置を介して認証代理装置が個人認証する個人認証システムを対象としている。

【0021】ここで、前記第1エンティティ装置は、前記秘匿通信の合意処理のメッセージを用い、前記ユーザの個人認証に関する本人確認仕様を前記通信代理装置に送信する手段と、この送信された本人確認仕様に対応して得られる前記ユーザの本人確認情報を暗号化した状態で前記通信代理装置に通知する手段とを備えている。

【0022】また、前記通信代理装置は、前記第1エンティティ装置から送信された本人確認仕様を前記認証代理装置に送信する手段と、この送信された本人確認仕様に関する前記認証代理装置の選択結果に基づき、前記第1エンティティ装置から通知された暗号化された本人確

認情報を前記認証代理装置に送信する手段と、前記認証代理装置から送信された本人確認結果が不正を示すとき、前記合意処理を中断する手段とを備えている。

【００２３】さらに、前記認証代理装置は、前記通信代理装置から送信された本人確認仕様のうち、予め設定されたセキュリティポリシーに合致する本人確認仕様を選択し、得られた選択結果を前記通信代理装置に送信する手段と、前記通信代理装置から通知された暗号化された本人確認情報を復号し、得られた復号結果に基づいて本人確認処理を実行し、得られた本人確認結果を前記通信代理装置に送信する手段とを備えている。

【００２４】従って、第２の発明は、第１の発明と同様の作用効果に加え、認証代理装置が個人認証を行なうので、ユーザ側に対してはプライバシーの保護を充実させ、第２エンティティ装置側に対しては個人認証に関する負荷を軽減させることができる。

【００２５】なお、第１及び第２の発明は、全ての装置からなる「システム」として表現されているが、これに限らず、全ての装置又は各装置毎の「システム」、「装置」、「方法」、「プログラム」又は「記憶媒体」等として表現してもよいことは言うまでもない。

【００２６】

【発明の実施の形態】以下、本発明の各実施形態について図面を参照しながら説明する。なお、以下の各実施形態では、具体的な秘匿通信の一例として、ＳＳＬ／ＴＬＳを好適なものとして、これを拡張した例を述べる。また、ＴＬＳの汎用拡張仕様は「TLS Extensions」に詳しい（[TLSE] S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen and T. Wright, "TLS Extensions", Internet-Draft, June 20, 2001, http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-tls-extensions-00.txt）。また、各メッセージタイプ等のコードは、特に規定せずに任意のものとしており、他の標準及び拡張タイプで使用しているコードと衝突しないものであればよい。

【００２７】（第１の実施形態）図１は本発明の第１の実施形態に係る個人認証システムの一例を示す模式図である。この個人認証システムは、本人確認装置１０を有するクライアント装置２０がネットワークNWを介してサービスプロバイダ装置３０に接続されている。サービスプロバイダ装置３０は、ネットワークNWに接続された認証サーバ装置４０と、この認証サーバ装置４０に接続された本人確認参照情報の記憶装置５０とから構成されている。

【００２８】ここで、本人確認装置１０は、本人確認用にユーザの生体的特徴を測定する本人確認部１１と、本人確認部１１の測定結果から本人確認情報を測定してクライアント装置２０に送出する本人確認制御部１２とを備えている。なお、本人確認情報は、ここでは生体情報を用いるが、これに限らず、使用する本人確認方式に対応する情報であればよい。

【００２９】クライアント装置２０は、サービスプロバイダから提供されるサービスを受ける側の装置であり、通常のコンピュータ機能及び通常の秘匿通信機能に加え、秘匿通信の合意処理のメッセージを用い、ユーザの個人認証に関する本人確認仕様を認証サーバ装置４０に送信する機能と、この送信された本人確認仕様に関する前記第２エンティティ装置の選択結果に基づき、秘匿通信の合意処理の最中に、本人確認装置１０から受けた本人確認情報を暗号化した状態で認証サーバ装置４０に通知する機能と、この通知した本人確認情報を認証サーバ装置４０が不正と判定し、合意処理の中断宣言を伴う警告メッセージを返信したとき、警告メッセージを出力する機能とをもっている。

【００３０】ここで、クライアント装置２０としては、例えば図２に示すように、本人確認装置１０からの本人確認情報を秘匿通信ソフトウェアSW_{20}に送出するオペレーションシステムOS_{20}と、このオペレーションシステムOS_{20}から受けた本人確認情報を用いて秘匿通信を実行するための秘匿通信ソフトウェアSW_{20}とを備えて構成してもよい。

【００３１】この場合、秘匿通信ソフトウェアSW20は、周知の秘匿通信プロトコル実現機能に加え、本人確認情報を暗号化して送信するための機能を有しており、入出力部２１、メッセージ制御部２２、セッション管理部２３、秘匿部（暗号化部２４ａ、圧縮部２４ｂ、データ認証部２４ｃ及び鍵交換部２４ｄ）２４、本人確認情報制御部２５、認証部２６、公開鍵検証部２７及びセキュリティポリシー部２８から構成される。なお、これらのうち、周知の機能以外の要素は、図２中に破線ｄ１で囲んだように、メッセージ制御部２２の一部、本人確認情報制御部２５及びセキュリティポリシー部２８の一部とすればよい。

【００３２】ここで、メッセージ制御部２２は、周知のメッセージ制御機能に加え、本人確認情報制御部２５から転送された暗号化本人確認情報に関するメッセージを制御可能なものである。

【００３３】なお、暗号化本人確認情報に関するメッセージとしては、例えば図３乃至図５に示す如き、クライアントハローメッセージM_{CH}及びクライアント確認メッセージM_{CA}がある。

【００３４】クライアントハロー（ClientHello）メッセージM_{CH}は、図３及び図４に示すように、プロトコルバージョンフィールドと、クライアント装置２０が生成したクライアントランダム（乱数：Random）と、セッションＩＤフィールドと、クライアント装置２０の対応している暗号化仕様（CipherSuites）と圧縮仕様（CompressionMethod）のリストとに加え、拡張フィールドMCH-EXTにて、クライアント装置２０が対応している本人確認仕様（AuthenticationMethod）のリスト（以下、ク

ライアント確認リスト（ClientAuthenticationList）という）とを含んでいる。

【００３５】クライアント確認（ClientAuthenticate）メッセージM_{CA}は、図５に示すように、プロトコルバージョンフィールド及び暗号化確認フィールドに加え、拡張フィールドとして、暗号化された本人確認情報を含む確認データ（AuthenticationData）フィールドと、生体認証方式に使用した本人確認仕様（AuthenticationMethod）フィールドとを含んでいる。

【００３６】本人確認情報制御部２５は、メッセージ制御部２２や秘匿部２４との間で、メッセージに含める本人確認情報の暗号化等を制御するためのものであり、具体的には、オペレーションシステムOS_{2c}から入出力部２１及びメッセージ制御部２２を介して受けた本人確認情報を秘匿部２４に転送して暗号化させる機能と、秘匿部２４により得られた暗号化本人確認情報をメッセージ制御部２２に転送する機能とをもっている。

【００３７】セキュリティポリシー部２８は、周知の秘匿通信のセキュリティポリシーに加え、本人確認に関するセキュリティポリシーが予め登録されたものである。

【００３８】一方、認証サーバ装置４０は、クライアント装置２０からの要求に応じてサービスを提供する側の装置であり、通常のコンピュータ機能及び通常の秘匿通信機能に加え、秘匿通信の合意処理の最中に、クライアント装置２０から受けたクライアントハローメッセージ内の本人確認リスト内の本人確認仕様を自装置のセキュリティポリシーに基づいて選択する機能と、選択した本人確認仕様に基づき、クライアント装置２０から受けるクライアント確認メッセージM_{CA}に含まれる暗号化本人確認情報を記憶装置５０内の本人確認参照情報を参照しながら検証する機能と、検証結果が不正を示すとき、秘匿通信の合意処理を中断する機能とをもっている。

【００３９】ここで、認証サーバ装置４０としては、例えば図６に示すように、通常のオペレーションシステムOS_{40}と、このオペレーションシステムOS_{40}に制御され、クライアント装置２０から受ける本人確認情報を検証して秘匿通信を実行するための秘匿通信ソフトウェアSW_{40}とを備えて構成してもよい。

【００４０】この場合、秘匿通信ソフトウェアSW_{40}は、周知の秘匿通信プロトコル実現機能に加え、暗号化された本人確認情報を復号して検証するための機能を有しており、入出力部４１、メッセージ制御部４２、セッション管理部４３、秘匿部（暗号化部４４ａ、圧縮部４４ｂ、データ認証部４４ｃ及び鍵交換部４４ｄ）４４、復号部４５、検証部４６、認証部４７、公開鍵検証部４８及びセキュリティポリシー部４９から構成される。なお、これらのうち、周知の機能以外の要素は、図６中に破線ｄ２で囲んだように、メッセージ制御部４２の一部、復号部４５、検証部４６、及びセキュリティポリシー部４９の一部とすればよい。

【００４１】ここで、メッセージ制御部４２は、周知のメッセージ制御機能に加え、クライアント装置２０から送信された暗号化本人確認情報に関するメッセージM_{CH}，M_{CA}等を制御可能なものである。

【００４２】復号部４５は、メッセージ制御部４２からクライアント確認メッセージM_{CA}内の暗号化本人確認情報を受けると、この暗号化本人確認情報を復号し、得られた本人確認情報を検証部４６に送出する機能をもっている。

【００４３】検証部４６は、復号部４５から送出された本人確認情報を、記憶装置５０の記憶内容を参照して検証し、検証結果が正当であれば秘匿通信を継続し、検証結果が不当であれば警告（Alert）メッセージを送信して秘匿通信を中断する機能をもっている。

【００４４】なお、検証部４６による検証は、例えば本人確認情報に指紋情報を用いた場合、本人確認参照情報を指紋テンプレートとして、送信された指紋情報と指紋テンプレートとの照合により、実行可能となっている。この場合、指紋情報は、生の画像情報でもよいが、通信負荷等を低減する観点から、予め本人確認装置１０側ではクライアント装置２０側で特徴抽出処理などを行なうことが好ましい。なお、ここでは、本人確認情報等の情報フォーマットは任意である。

【００４５】セキュリティポリシー部４９は、周知の秘匿通信のセキュリティポリシーに加え、本人確認に関するセキュリティポリシーが予め登録されたものである。

【００４６】記憶装置５０は、認証サーバ装置４０から読出可能に制御され、本人確認情報を検証するために基準となる情報であるユーザ個人の本人確認参照情報が記憶されている。本人確認参照情報は、例えば本人確認方式が生体認証の場合、生体情報テンプレートなどが使用可能であるが、これに限らず、使用する本人確認方式に対応する基準情報であればよい。

【００４７】次に、以上のように構成された個人認証システムの動作を図７のシーケンス図を用いて説明する。クライアント装置２０は、セッション確立要求をサービスプロバイダの認証サーバ装置４０に送信する（ＳＴ１）。

【００４８】認証サーバ装置４０は、セッション確立要求を受けると、ハンドシェイク（Handshake）開始を宣言するハロー要求（HelloRequest）メッセージをクライアント装置２０に送信する（ＳＴ２）。

【００４９】クライアント装置２０は、ハロー要求メッセージを受けると、本人確認情報の暗号化に関するクライアントランダム、暗号化仕様及び圧縮仕様のリストと、クライアント確認リストとを含むクライアントハローメッセージM_{CH}を認証サーバ装置４０に送信する（ＳＴ３）。

【００５０】認証サーバ装置４０は、クライアントハローメッセージM_{CH}を受けると、このメッセージM_{CH}内の

クライアント確認リストに含まれる複数の本人確認仕様のうち、提供サービスが要求する本人確認仕様を選択すると共に、暗号化仕様及び圧縮仕様を選択し、サーバランダム（乱数）を生成する。なお、認証サーバ装置４０は、セキュリティポリシー部２８の登録内容に基づいて本人確認仕様を選択するが、１つの方式に限らず、複数の方式を選択してもよい。

【００５１】しかる後、認証サーバ装置４０は、選択した本人確認仕様を有する本人確認フィールドと、暗号化仕様、圧縮仕様及びサーバランダムを含む拡張フィールドとを含むサーバハロー（ServerHello）メッセージをクライアント装置４０に送信する（ＳＴ４）。

【００５２】これにより、クライアント装置２０と認証サーバ装置４０との間で本人確認仕様の合意を確立できる。

【００５３】以下のステップＳＴ５～ＳＴ９の鍵交換処理及び公開鍵証明書検証処理は、周知技術なので説明を省略するが、その詳細はＲＦＣ２２４６に開示されている（[TLS] T. Dierks and C. Allen, "The TLS Protocol Version 1.0", RFC 2246,January 1999, http://www.ietf.cnri.reston.va.us/rfc/rfc2246.txt）。

【００５４】なお、ステップＳＴ６のサーバ鍵交換（ServerKeyExchange）メッセージは、証明書（Certificate）メッセージで提示する公開鍵証明書が署名のみにしか利用できない等の場合、鍵交換用の公開情報（ＲＳＡ公開鍵など）の送信用にオプションとして利用可能となっている。また、他のオプショナルのメッセージは、本実施形態では基本的に利用するものとする。

【００５５】次に、ステップＳＴ１０の本人確認情報の送信動作を説明する。

【００５６】クライアント装置２０は、本人確認情報を暗号化及び圧縮する仕様として、クライアントハローメッセージM_{CB}及びサーバハローメッセージによって合意したものを使用する。

【００５７】また、クライアント装置２０は、本人確認情報を暗号化する鍵（必要なら加えて初期ベクタ）等のパラメータを、標準状態で使用する主要パラメータ（例、クライアント／サーバ書込ＭＡＣシークレット、クライアント／サーバ書込キー、クライアント／サーバ書込初期ベクタ等）と同様に生成する。

【００５８】すなわち、クライアント装置２０は、サーバランダム、クライアントランダム及びプリマスターシークレットを用い、ハッシュアルゴリズムに基づいて、本人確認情報の暗号化鍵を生成する。

【００５９】具体的には、サーバランダム、クライアントランダム及びプリマスターシークレットを暗号化部２４ａの擬似乱数生成関数（pseudo-random function：ＰＲＦ）に入力し、得られた値をマスターシークレットとする。

【００６０】次に、マスターシークレット、サーバランダム及びクライアントランダムを同様に疑似乱数生成関数ＰＲＦに入力して得られた値をキーブロックとして、このキーブロックを必要なサイズに分割して、各パラメータを得る。

【００６１】このとき、周知の秘匿通信プロトコルでは、本来余分なキーブロックを破棄するが、ここでは本人確認情報暗号化用パラメータ（書込キー、書込初期ベクタ）分を余分なキーブロックとして生成する。

【００６２】しかる後、クライアント装置２０は、このようにして得た暗号化用パラメータに基づいて本人確認情報を暗号化し、暗号化本人確認情報を得る。

【００６３】暗号化本人確認情報は、図６に示したように、確認データフィールド（AuthenticationData）に格納され、クライアント確認メッセージM_{CA}内に保持されて認証サーバ装置４０に送信される（ＳＴ１０）。

【００６４】認証サーバ装置４０は、クライアント確認メッセージM_{CA}内の暗号化本人確認情報を、共有した本人確認情報暗号化用パラメータに基づいて復号し、得られた本人確認情報を記憶装置５０内の本人確認参照情報により検証する。

【００６５】ここで、認証サーバ装置４０は、検証結果が不当であれば、中断宣言を伴う警告（Alert）メッセージをクライアント装置２０に送信してセッションを中断し、検証結果が正当であればステップＳＴ１１～ＳＴ１５の周知のシーケンスを実行する。

【００６６】ステップＳＴ１５の完了後、クライアント装置２０は、サービスプロバイダからサービスが提供され、認証サーバ装置４０との間でアプリケーションデータを送受信する（ＳＴ１６）。

【００６７】上述したように本実施形態によれば、それぞれ秘匿通信機能を有した認証サーバ装置４０とクライアント装置２０との間での秘匿通信を行う際に、秘匿通信合意処理のメッセージを用いてユーザ個人が本人であるか否かを認証サーバ装置４０が確認できるので、秘匿通信の際に、第三者の成り済ましを阻止することができる。

【００６８】また、複数の本人確認仕様（本人確認手段）が存在する場合、接続される側が自己のセキュリティポリシーに従った本人確認仕様を選択できるので、個人認証の信頼性を向上させることができる。

【００６９】（第２の実施形態）図８は本発明の第２の実施形態に係る個人認証システムの一例を示す模式図であり、前述した図面と同一部分には同一符号を付し、変形した部分には同一符号にアルファベットの添字を付してその同一部分の説明を省略し、ここでは変形した部分について主に述べる。なお、他の図面についても同様にして重複した説明を省略する。

【００７０】すなわち、本実施形態は、第１の実施形態の変形例であり、ユーザ側からはプライバシーの保護の充実を図り、サービスプロバイダ側からは管理の負荷の

軽減を図るものとして、ユーザの本人確認参照情報や測定情報に関し、通信処理や認証処理を専用の代理サーバ装置に分担させたものである。

【００７１】具体的には、前述した認証サーバ装置４０を変形し、通信端点間の通信経路の中間に位置して通信を中継する通信代理サーバ装置４０ａと、認証を代理する認証代理サーバ装置４０ｂと、サービスを提供するサービスプロバイダ装置４０ｃとを備え、図中①～⑫の順に秘匿通信が接続されるものとなっている。

【００７２】これに伴い、前述したクライアント装置２０を変形し、これら３種類の装置４０ａ～４０ｃに通信可能なクライアント装置２０ａとしている。

【００７３】ここで、クライアント装置２０ａは、前述した秘匿通信合意処理の機能において、全ての通信を通信代理装置４０ａを介して送信先に送信する機能と、認証代理サーバ装置４０ｂのＵＲＬを含む認証ＵＲＬ（AuthenticateURL）メッセージM_{AURL}を通信代理サーバ装置４０ａに通知する機能とをもっている。

【００７４】認証ＵＲＬメッセージM_{AURL}は、図９に示すように、クライアント装置２０ａのプロトコルバージョンを格納するプロトコルバージョン（ProtocolVersion）フィールドと、認証代理サーバ装置４０ｂのＵＲＬ（Uniform Resource Locators）を格納する認証サーバＵＲＬ（AuthenticationServerURL）フィールドと、本人確認情報を暗号化するための暗号化パラメータ（暗号化鍵と必要ならば初期ベクタ）を認証代理サーバ装置４０ｂの公開鍵で暗号化したものを格納する暗号化一時鍵（EncryptedTempKey）フィールドと、上記各フィールドに対してクライアント装置２０ａの秘密鍵（クライアント装置２０ａの公開鍵証明書と対となる鍵）で施したデジタル署名を格納する署名（Signature）フィールドとから構成される。

【００７５】このデジタル署名の署名対象項目には、リプレイ攻撃を防止する観点から、署名作成日時を示したタイムスタンプ（Timestamp）を加えてもよく、また、クライアントランダムとサーバランダムを加えてもよい。各項目を加える場合、加える項目を認証ＵＲＬメッセージM_{AURL}内に含める。

【００７６】暗号化パラメータは、クライアント装置２０ａで生成してもよいが、プリマスタシークレットと同フォーマットの値を送信してもよい。同フォーマットの値を送信する場合、クライアントランダムとサーバランダムを認証ＵＲＬメッセージM_{AURL}の項目として送信し、通常の通信パラメータ生成処理と同様に暗号化パラメータを送信してもよい。

【００７７】一方、通信代理サーバ装置４０ａは、クライアント装置２０ａとサービスプロバイダ装置４０ｃとの間の秘匿通信合意処理に関し、クライアント装置２０ａ側の通信処理を代理する機能を有している。

【００７８】具体的には、通信代理サーバ装置４０ａは、クライアント装置２０ａとの間の秘匿通信合意処理の途中で、クライアント装置２０ａから受けた認証ＵＲＬメッセージM_{AURL}に基づいて、認証代理サーバ装置４０ｂと秘匿通信合意処理を行なう機能と、クライアント装置２０ａから受けた本人確認情報を含むクライアント確認メッセージM_{CA}を認証代理サーバ装置４０ｂに送信して本人確認をしてもらう機能と、認証代理サーバ装置４０ｂから受けたサーバ確認結果メッセージM_{SAR}内の本人確認結果が正当性を示すとき、クライアント装置２０ａとの間の秘匿通信合意処理を継続して完了する機能と、このサーバ確認結果メッセージM_{SAR}内の本人確認結果が不正を示すとき、クライアント装置２０ａとの間の秘匿通信合意処理を中断する機能とをもっている。

【００７９】また、通信代理サーバ装置４０ａは、クライアント装置２０ａとの秘匿通信合意処理の完了後、サービスプロバイダ装置４０ｃとの間の秘匿通信合意処理を実行する機能と、この秘匿通信合意処理中に、認証代理サーバ装置４０ｂによる本人確認結果を示すクライアント確認結果メッセージM_{CAR}をサービスプロバイダ装置４０ｃに送信する機能とをもっている。

【００８０】ここで、サーバ確認結果（ServerAuthenticateResult）メッセージM_{SAR}は、図１０及び図１１に示すように、本人確認結果を示す確認結果（AuthenticateResult）フィールドと、本人確認処理の情報を格納する確認情報（AuthenticateInfo）フィールドM_{SAR-AI}と、上記各項目に対して認証代理サーバ装置４０ｂの秘密鍵で施したデジタル署名である署名フィールドから構成される。

【００８１】確認情報フィールドM_{SAR-AI}は、本人確認手段に応じて種々の情報のフィールドを設定可能であり、図１１の例では、クライアント装置名、本人確認仕様、タイムスタンプ、認証者名及びマックスエイジ等の各フィールドが使用されている。

【００８２】ここで、クライアント装置名（ClientName）フィールドは、クライアント装置名を示し、本人確認仕様（AuthenticationMethod）フィールドは、使用した本人確認手段を示す。タイムスタンプ（Timestamp）フィールドは認証代理サーバ装置４０ｂによる本人確認処理の時刻を示し、認証者名（AuthenticatorName）フィールドは認証代理サーバ装置名を示す。マックスエイジ（MaxAge）フィールドは、本人確認結果の有効期限（生存時間）を示す。

【００８３】クライアント確認結果（ClientAuthenticateResult）メッセージM_{CAR}は、図１２に示すように、認証代理サーバ装置４０ｂより送信された本人確認結果であるサーバ確認結果メッセージM_{SAR}の各項目により構成される。

【００８４】認証代理装置４０ｂは、通信代理サーバ装置４０ａからの秘匿通信の合意処理の最中に、通信代理サーバ装置４０ａから受けたクライアントハローメッセ

ージM_{CH}内の本人確認リスト内の本人確認仕様を予め設定されたセキュリティポリシーに基づいて選択する機能と、選択した本人確認仕様に基づき、通信代理サーバ装置４０ａから受ける認証代理メッセージM_{AR}に含まれる本人確認情報と記憶装置５０内の本人確認参照情報とを照合して本人確認処理を行なう機能と、本人確認結果を含むサーバ確認結果メッセージM_{SAR}を通信代理サーバ装置４０ａに送信する機能とをもっている。

【００８５】なお、認証代理サーバ装置４０ｂは、本人確認処理以外の本人確認処理に付随する保証処理を有していてもよい。すなわち、本人確認に使用する本人確認を行うデバイスの正当性を保証又は認証してもよい。

【００８６】サービスプロバイダ装置４０ｃは、通信代理サーバ装置４０ａと秘匿通信合意処理を行なう機能と、この秘匿通信合意処理の最中に、通信代理サーバ装置４０ａから受けたクライアント確認結果メッセージM_{CAR}に含まれる本人確認結果を検証する機能と、本人確認結果が正当性を示すとき、通信代理サーバ装置４０ａとの秘匿通信合意処理の完了に伴い、通信代理サーバ装置４０ａを介してクライアント装置２０ａにサービスを提供する機能とをもっている。

【００８７】次に、以上のように構成された個人認証システムの動作を図８の①～㉔に示す接続順序に従い、図１３乃至図１５のシーケンス図を用いて説明する。

【００８８】［①：クライアント装置２０ａ－通信代理サーバ装置４０ａ間］クライアント装置２０ａは、前述同様に、サービスプロバイダ側にセッション確立要求を送信する（ＳＴ１）。

【００８９】但し、クライアント装置２０ａの通信ソフトウェアは、予め送信内容が通信代理サーバ装置４０ａを介して送信先に届くように設定されている。この設定は、ＷＷＷブラウザの場合での一般的なプロキシ設定と同様であり、通信プロトコル毎にＩＰアドレスや接続ポート等が設定される。本実施形態では、ＨＴＴＰＳ接続の場合、通信代理サーバ装置４０ａを介するように通信代理サーバ装置４０ａのＩＰアドレスと接続ポートが予め設定される。

【００９０】いずれにしても、この設定により、クライアント装置２０ａは、ステップＳＴ１のセッション確立要求を通信代理サーバ装置４０ａに送信し、秘匿通信合意処理を開始する。

【００９１】この秘匿通信合意処理は、全体的には、図７に示したステップＳＴ１～ＳＴ１５と同様に実行される。但し、ステップＳＴ９の完了後でステップＳＴ１０の開始前に、クライアント装置２０ａは、認証代理サーバ装置４０ｂのＵＲＬや暗号化パラメータ等を含む認証ＵＲＬメッセージM_{AURL}を通信代理サーバ装置４０ａに送信する（ＳＴ１０ａ）。

【００９２】これにより、本人確認参照情報を有する認証代理サーバ装置４０ｂのＵＲＬ等が通信代理サーバ装置４０ａに通知される。

【００９３】以下、前述同様に、ステップＳＴ１０，ＳＴ１１が実行された後、クライアント装置２０ａと通信代理サーバ装置４０ａとの間の秘匿通信合意処理が一旦、保留され、通信代理サーバ装置４０ａは、以下に述べるように、認証代理サーバ装置４０ｂに対し、秘匿通信合意処理の際に、本人確認情報を検証してもらう。

【００９４】［㉒：通信代理サーバ装置４０ａ－認証代理サーバ装置４０ｂ間］通信代理サーバ装置４０ａは、クライアント装置２０ａとの秘匿通信合意処理の途中に、認証ＵＲＬメッセージM_{AURL}内のＵＲＬを用いて、セッション確立要求を認証代理サーバ装置４０ｂに送信し（㉒㉓のＳＴ１）、認証代理サーバ装置４０ｂとの間で秘匿通信合意処理を開始する。

【００９５】この秘匿通信合意処理も全体的には、図７に示したステップＳＴ１～ＳＴ１１と同様に実行される。但し、ステップＳＴ９の完了後でステップＳＴ１０の開始前に、通信代理サーバ装置４０ａは、認証ＵＲＬメッセージM_{AURL}とクライアント確認メッセージM_{CA}との内容を含む認証代理メッセージM_{AR}を認証代理サーバ装置４０ｂに送信する（ＳＴ１０ｂ）。

【００９６】これにより、暗号化パラメータや暗号化本人確認情報等が認証代理サーバ装置４０ｂに通知されることになる。

【００９７】すなわち、認証代理サーバ装置４０ｂは、認証代理メッセージM_{AR}を受けると、署名フィールドをクライアント装置２０ａの公開鍵で検証する。正当性が証明されたら、暗号化一時鍵フィールドを認証代理サーバ装置４０ｂの秘密鍵で復号をして、本人確認情報を復号するための暗号化パラメータを取得する。また、取得した暗号化パラメータにより本人確認情報である暗号化確認フィールドを復号し、本人確認情報と本人確認仕様を取得する。

【００９８】しかる後、認証代理サーバ装置４０ｂは、本人確認情報と記憶装置５０内の本人確認参照情報とを照合して本人確認情報を検証する。検証の結果、本人であると確認された場合、ステップＳＴ１１の後に、認証代理サーバ装置４０ｂは、本人確認結果を示すサーバ確認結果メッセージM_{SAR}を通信代理サーバ装置４０ａに送信する（ＳＴ１１ｂ）。

【００９９】通信代理サーバ装置４０ａは、サーバ確認結果メッセージM_{SAR}を受信すると、終了メッセージを認証代理サーバ装置４０ｂに送信し（ＳＴ１１ｂ１）、折り返し、終了メッセージを認証代理サーバ装置４０ｂから受信して（ＳＴ１１ｂ２）、認証代理サーバ装置４０ｂとの間の通信を終了する。

【０１００】続いて、通信代理サーバ装置４０ａは、サーバ確認結果メッセージM_{SAR}内の本人確認結果が正当である場合、クライアント装置２０ａに対して暗号仕様交換（ＣｈａｎｇｅＣｉｐｈｅｒＳｐｅｃ）メッセージ以下のシーケンス

を続行する（①側のＳＴ１２～ＳＴ１５）。

【０１０１】一方、本人確認結果が正当でない場合、通信代理サーバ装置４０ａは、中断宣言を伴う警告（Alert）メッセージをクライアント装置２０ａに送信し、セッションの中断を宣言する。

【０１０２】以上により、クライアント装置２０ａと通信代理サーバ装置４０ａとの間の秘匿通信合意処理が完了する。但し、アプリケーションデータの送受信は、以下の通信代理サーバ装置４０ａとサービスプロバイダ装置４０ｃのセッションが確立された後に行われる。

【０１０３】［⑬：通信代理サーバ装置４０ａ－サービスプロバイダ装置４０ｃ間］クライアント装置２０ａとの秘匿通信合意処理の完了後、通信代理サーバ装置４０ａは、図１４に示すように、ステップＳＴ１のセッション確立要求をサービスプロバイダ装置４０ｃに送信し（⑬側のＳＴ１）、サービスプロバイダ装置４０ｃとの間で秘匿通信合意処理を開始する。

【０１０４】この秘匿通信合意処理も全体的には、図７に示したステップＳＴ１～ＳＴ１５と同様に実行される。但し、ステップＳＴ１０のクライアント確認メッセージに代えて、クライアント確認結果メッセージM_{CAR}が用いられる。

【０１０５】すなわち、通信代理サーバ装置４０ａは、ステップＳＴ９の後、本人確認結果を含むクライアント確認結果メッセージM_{CAR}をサービスプロバイダ装置４０ｃに送信する（ＳＴ１０ｃ）。

【０１０６】サービスプロバイダ装置４０ｃは、このクライアント確認結果メッセージM_{CAR}の署名フィールドを認証代理サーバ装置４０ｂの公開鍵証明書で検証し、メッセージの正当性を検証する。正当性を確認すると、確認結果フィールドにより本人確認結果を取得する。

【０１０７】以下、図７と同様に、ステップＳＴ１１～ＳＴ１５のシーケンスが実行され、ステップＳＴ１５の終了により、通信代理サーバ装置４０ａとサービスプロバイダ装置４０ｃとの間の秘匿通信合意処理が完了する。

【０１０８】従って、クライアント装置２０ａと通信代理サーバ装置４０ａとの間、及び通信代理サーバ装置４０ａとサービスプロバイダ装置４０ｃとの間において、秘匿通信路の構築が完了する。

【０１０９】［⑭：クライアント装置２０ａ－サービスプロバイダ装置４０ｃ間］各装置間の秘匿通信路の構築完了後、クライアント装置２０ａは、図１４に示すように、通信代理サーバ装置４０ａを介してサービスプロバイダ装置４０ｃとの間でアプリケーションデータを送受信し（ＳＴ１６）、サービスの提供を受ける。

【０１１０】上述したように本実施形態によれば、第１の実施形態と同様の効果に加え、認証代理サーバ装置４０ｂが個人認証を行なうので、サービスプロバイダ装置４０ｃ側に対しては個人認証に関する負荷を軽減させ、ユーザ側に対してはプライバシーの保護を充実させることができる。

【０１１１】例えば、生体情報は、パスワードのような選択的な秘密情報とは異なり、個人固有の生体の特徴を表すため、個人のプライバシーを考慮して取扱う必要があるが、本実施形態によれば、本人確認参照情報や本人確認情報をサービスプロバイダ装置４０ｃに開示せず、本人確認結果のみをサービスプロバイダ装置４０ｃに開示するので、ユーザ個人のプライバシーの保護を充実できる。

【０１１２】また、認証代理サーバ装置４０ｂを複数のサービスプロバイダ間で共用することにより、本人確認処理で用いる生体情報テンプレートなどの本人確認参照情報を一元的に扱うことができ、かつその本人確認結果を再利用することができる。

【０１１３】なお、第２の実施形態においては、通信代理サーバ装置４０ａと認証代理サーバ装置４０ｂを同一装置内に設けてもよい。その場合、図１３の②に示す通信シーケンスは省略され、認証代理サーバ装置４０ｂにて行われる各処理を通信代理サーバ装置４０ａで行えばよい。

【０１１４】図１３の②に示す通信シーケンス②は一例であり、これに限らず、別途安全な通信路上を上記各メッセージと同機能を有するメッセージを送受信する構成に変形してもよい。すなわち、秘匿通信のアプリケーションデータとして上記認証代理メッセージM_{AR}及びサーバ確認結果メッセージM_{SAR}と同様な項目構成をもつメッセージを送受信すればよい。

【０１１５】また、本人確認情報及び本人確認結果を通知するメッセージを秘匿通信合意処理外にて（アプリケーションデータとして）送信してもよい。すなわち、秘匿通信通知手段を単独で動作させてもよい。

【０１１６】なお、上記第１及び第２の実施形態では、秘匿通信プロトコルとしてＳＳＬ／ＴＬＳを適用した例を説明したが、これに限らず、他の秘匿通信プロトコルを用いた構成に変形しても、本発明を同様に実施して同様の効果を得ることができる。

【０１１７】同様に、上記第１及び第２の実施形態では、「サービスプロバイダ」の語を用いたが、これは民間業者に限らず、電子政府等の官公庁のサービス提供業務に具体化しても、本発明を同様に実施して同様の効果を得ることができる。

【０１１８】また、第１の実施形態では、「第１エンティティ装置」をクライアント装置２０とし、「第２エンティティ装置」を認証サーバ装置４０とした場合について説明したが、これに限らず、例えば第１及び第２エンティティ装置の両者ともがユーザ端末装置である場合でも、本発明を同様に実施して同様の効果を得ることができる。

【０１１９】なお、上記各実施形態に記載した手法は、

コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（CD-ROM、DVDなど）、光磁気ディスク（MO）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【0120】また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【0121】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【0122】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0123】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0124】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0125】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0126】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成用件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【0127】その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0128】

【発明の効果】以上説明したように本発明によれば、秘匿通信の際に、第三者の成り済ましを阻止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る個人認証システムの一例を示す模式図。

【図2】同実施形態におけるクライアント装置及びその周辺構成を示す機能ブロック図。

【図3】同実施形態におけるクライアントハローメッセージの例を示すメッセージ構造図。

【図4】同実施形態における拡張フィールドの例を示すデータ構造図。

【図5】同実施形態におけるクライアント確認メッセージの例を示すメッセージ構造図。

【図6】同実施形態における認証サーバ装置及びその周辺構成を示す機能ブロック図。

【図7】同実施形態における動作を説明するためのシーケンス図。

【図8】本発明の第2の実施形態に係る個人認証システムの一例を示す模式図。

【図9】同実施形態における認証URLメッセージの例を示すメッセージ構造図。

【図10】同実施形態におけるサーバ確認結果メッセージの例を示すメッセージ構造図。

【図11】同実施形態における確認情報フィールドの例を示すデータ構造図。

【図12】同実施形態におけるクライアント確認結果メッセージの例を示すメッセージ構造図。

【図13】同実施形態における動作を説明するためのシーケンス図。

【図14】同実施形態における動作を説明するためのシーケンス図。

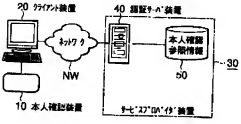
【符号の説明】

10…本人確認装置10
11…本人確認部11
12…本人確認制御部12
20，20a…クライアント装置20
OS_{20}…オペレーションシステム
SW_{20}…秘匿通信ソフトウェア
21，41…入出力部21
22，42…メッセージ制御部22
23，43…セッション管理部23
24，44…秘匿部24
24a，44a…暗号化部24a
24b，44b…圧縮部24b
24c，44c…データ認証部24c
24d，44d…鍵交換部24d
25…本人確認情報制御部25
26，47…認証部26
27，48…公開鍵埃証部27
28，49…セキュリティポリシー部28
30，40c…サービスプロバイダ装置30
40…認証サーバ装置40

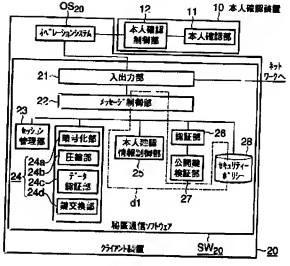
45…復号部
46…検証部
40a…通信代理サーバ装置
40b…認証代理サーバ装置
50…記憶装置50
NW，NW1，NW2…ネットワークNW
d1，d2…破線

M_{CH}…クライアントハローメッセージ
M_{CH-EXT}…拡張フィールド
M_{CA}…クライアント確認メッセージ
M_{AURL}…認証URLメッセージ
M_{SAR}…サーバ確認結果メッセージ
M_{SAR-AI}…確認情報フィールド
M_{CAR}…クライアント確認結果メッセージ

【図1】



【図2】



【図3】

【図4】

M_{CH} クライアントハローメッセージ

```
struct {
        ProtocolVersion client_version;
        Random random;
        SessionID session_id;
        CipherSuite cipher_suites;
        CompressionMethod compression_methods;
        Extension client_hello_extension_list;
}ClientHello;

struct {
        ExtensionType extensionType;
        opaque extension_data;
}Extension;
```

M_{CH-EXT}

M_{CH-EXT} 拡張フィールド

```
enum {
        client_auth;
}ExtensionType;

enum{
        uint8 AuthenticationMethod[2];
}ExtensionData;
```

【図5】

M_{CA} クライアント確認メッセージ

```
struct {
        ProtocolVersion client_version;
        EncryptedAuthentication encrypted_authentication;
}ClientAuthenticate;

struct {
        AuthenticationMethod authentication_method;
        AuthenticationData authentication_data;
}encrypted_authentication;
```

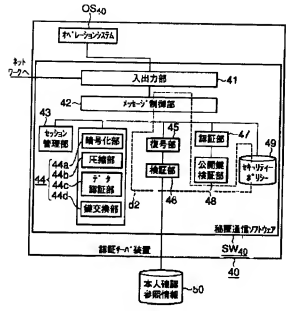
【図10】

M_{SAR} サーバ確認結果メッセージ

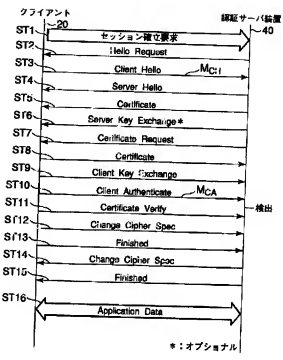
```
struct {
        ProtocolVersion client_version;
        AuthenticateResult authenticate_result;
        AuthenticateInfo authenticate_Info;
        Signature signature;
}ServerAuthenticateResult;
```

M_{SAR-AI}

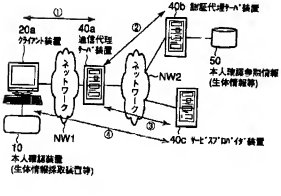
【図6】



【図7】



【図8】



【図9】

MAURL 認証URLメッセージ

```
struct {
        ProtocolVersion client_version;
        AuthenticationServerURL authentication_server_url;
        EncryptedTempKey encrypted_temp_key;
        Signature signature;
}AuthenticateURL;

struct {
        TemporaryKey temporary_key;
}encrypted_temp_key;
```

【図11】

MSAR-AI 認証情報フィールド

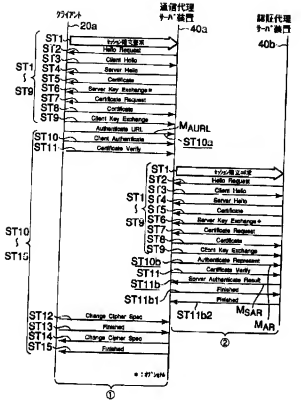
```
struct {
        ProtocolVersion server_version;
        ClientName client_name;
        AuthenticationMethod authentication_Method;
        Timestamp timestamp;
        AuthenticatorName authenticator_name;
        MaxAge max_age;
}AuthenticateInfo;
```

【図12】

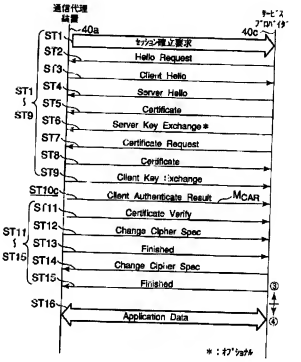
MCAR クライアント認証結果メッセージ

```
struct {
        ProtocolVersion client_version;
        AuthenticateResult authenticate_result;
        AuthenticateInfo authenticate_info;
        Signature signature;
}ClientAuthenticateResult;
```

【図１３】



【図１４】



フロントページの続き

(72)発明者　才所　敏明
東京都府中市東芝町１番地　株式会社東芝
府中事業所内